UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,954	11/17/2003	Peter D. Baker	705593.4001	4464

34313 7590 04/09/2007

ORRICK, HERRINGTON & SUTCLIFFE, LLP
IP PROSECUTION DEPARTMENT
4 PARK PLAZA
SUITE 1600
IRVINE, CA 92614-2558

EXAMINER	
JEAN GILLES, JUDE	
ART UNIT	**PAPER NUMBER**
2143	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/715,954	BAKER ET AL.	
	Examiner	Art Unit	
	Jude J. Jean-Gilles	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/14/2005, and 09/07/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Action is in regards to application number 10/715954 filed on 11/17/2003.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 1-20,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Maari, U.S. Patent No. 7,120,604 B2 in view of Baker et al et al (Baker), U.S. Patent No 6,493,761 B1.

Regarding **claim 1**, Maari teaches the invention substantially as claimed. Maari discloses a method of securely distributing digital content a (figs. 1, 4, and 5), comprising:

receiving a content distribution request from a content user (column 7, lines 19-23);

retrieving a digital content item in response to the content distribution request (column 7, lines 29-37);

generating a first encryption algorithm for encrypting the digital content item (column 7, lines 29-37; column 40, lines 27-39; *Note that Encoding is the process of converting one digital format to another, applying known algorithms to either obscure the content of the file, or to compress or convert it to another format*); and

transmitting the encrypted digital content item to the content user (column 7, lines 19-37; column 34, lines 1-8). However Maari does not specifically disclose the steps of "configuring a protocol parsing engine to encrypt the digital content item, using the first encryption algorithm; and encrypting the digital content item using the configured protocol parsing engine"

In the same field of endeavor, Baker discloses a method in which "*...Systems and methods for data processing using a protocol parsing engine...[see Baker, title and abstract]... and specifically a method for parsing data according to configurable criteria, the method comprising steps of: storing in a first data storage device a plurality of programmably configurable protocol descriptions that define a plurality of control character characteristics of the data; storing in a second data storage device a program for controlling a data parsing function to be executed by a processing unit, the program including instructions for causing the processing unit to selectively retrieve at least one of the programmably configurable protocol descriptions from the first data storage device and to vary the execution of the data parsing function based upon the at least one retrieved protocol description file; delivering the program for controlling the data parsing function to the processing unit; delivering the data to the processing unit; and enabling the processing unit to execute the data parsing function...[see Baker; column 51, lines 51-67].*

Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Baker's teachings of a method using configuring a protocol parsing engine to encrypt the digital content item,

using the first encryption algorithm, with the teachings of Maari, for the purpose of "*...providing a to improved systems and methods for parsing, searching, filtering, gathering statistics, and converting data files generated by any data editor, using character sets and editor controls definitions that can be programmably defined* ..." as stated by Baker in lines 65-67 of column 2, and lines 1-9 of column 3. By this rationale **claim 1** is rejected.

Regarding claims 2-20, the combination of Maari–Baker discloses:

2. The method of claim 1, further comprising generating a first encryption key (see Maari; column 6, lines 5-26).

3. The method of claim 2, wherein the configuring step further comprises using the first encryption key (see Maari; column 6, lines 5-26).

4. The method of claim 1, further comprising recording an encryption identifier adapted to identify the first encryption algorithm (see Maari; column 6, lines 5-26).

5. The method of claim 1, wherein the first encryption algorithm is different from a second encryption algorithm, the second encryption algorithm being a previously generated encryption algorithm used to encrypt a second digital content item transmitted to a second content user (see Maari; column 24, lines 54-67).

6. The method of claim 1, wherein generating the encryption algorithm comprises retrieving the encryption algorithm from a pool of encryption algorithms (see Maari; column 6, lines 5-26).

7. A method of securely accessing encrypted digital content, comprising:
requesting from a content provider access to encrypted digital content (see Maari; column 7, lines 19-23);
receiving decryption information from the content provider (see Maari; column 5, lines 3-13; column 42, lines 1-5);
decrypting the encrypted digital content using the decryption information (see Maari; column 5, lines 3-13; column 42, lines 1-23; [see Baker; column 51, lines 51-67]);
accessing the decrypted digital content (see Maari; column 5, lines 3-13; column 42, lines 1-23); and
deleting the decryption information (see Maari; column 8, lines 21-33).

8. The method of claim 7, wherein the encrypted digital content is stored locally (see Maari; column 7, lines 19-39).

9. The method of claim 7, wherein the decryption information comprises an executable decryption code module (see Maari; column 8, lines 5-16).

10. The method of claim 9, wherein the executable decryption code module is created

on demand by the content provider [see Baker; column 51, lines 51-67].

11. The method of claim 10, wherein the executable decryption code module is created by a protocol description configured to generate executable code [see Baker; column 51, lines 51-67].

12. The method of claim 7, wherein the received decryption information is stored in volatile memory [see Baker; column 51, lines 51-67].

13. The method of claim 7, wherein the decrypted digital content is stored in volatile memory [see Baker; column 51, lines 51-67].

14. The method of claim 7, further comprising deleting the decrypted digital content once it has been accessed (see Maari; column 7, lines 19-37; column 34, lines 1-8)..

15. The method of claim 7, further comprising receiving encryption information from the content provider and re-encrypting the decrypted digital content, using the encryption information (see Maari; column 5, lines 3-13; column 42, lines 1-23).

16. The method of claim 15, wherein the encryption information is different from second encryption information used to initially encrypt the decrypted digital content (see Maari; column 5, lines 3-13; column 42, lines 1-23).

17. A method of providing secure access to encrypted digital content, comprising: receiving a request to access encrypted digital content; retrieving a decryption algorithm for decrypting the encrypted digital content (see Maari; column 7, lines 19-29); configuring a protocol description to generate a code module for decrypting the encrypted digital content, using the decryption algorithm [see Baker; column 51, lines 51-67; see also abstract and title];
generating the code module for decrypting the encrypted digital content, using the configured protocol description [see Baker; column 51, lines 51-67; see also abstract and title];
transmitting the code module to the content user (see Maari; column 7, lines 19-37; column 34, lines 1-8)..

18. The method of claim 17, wherein the code module comprises an executable code module (see Maari; column 7, lines 19-37; column 34, lines 1-8)..

19. The method of claim 17, wherein the request to access encrypted digital content comprises an identifier identifying the digital content (see Maari; column 6, lines 5-26).

20. The method of claim 19, wherein retrieving the decryption algorithm comprises regenerating a decryption algorithm, based on the identifier (see Maari; column 5, lines 3-13; column 42, lines 1-23).

Conclusion

3. **THIS ACTION IS MADE NON-FINAL**. The Examiner strongly anticipates a Final Rejection Office Action on the next response if amendments are not properly made to the claims to perhaps place them in condition for allowance.

Any inquiry concerning this communication or earlier communications from examiner should be directed to Jude Jean-Gilles whose telephone number is (571) 272-3914. The examiner can normally be reached on Monday-Thursday and every other Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Wiley, can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-9000.

Jude Jean-Gilles

Patent Examiner

Art Unit 2143

JJG

March 26, 2007

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100